セキュアOSと仮想マシンを利用した情報漏洩とウィルス侵入の防止

鮫島吉喜　才所秀明
日立ソフトウェアエンジニアリング株式会社

要旨

機密情報を扱うWindows環境とインターネットにアクセス可能でウィルス感染の可能性があるWindows環境を，セキュアOSと仮想マシンを使って一台のPCに統合した二系統Windowsシステムを報告する．情報を扱う環境を仮想物理レベルから分離したことで，未知のウィルスが現れても，被害はインターネットにアクセス可能なWindows環境に止まり，機密情報がインターネットに漏洩することはない．本稿では，システム概要，セキュアOSを用いた安全性向上策，性能の他，安全性の検討を報告する．

Prevention of Information Leakage and Virus Infection with use of Secure OS and Virtual Machine

Yoshiki Sameshima　Hideaki Saisho
Hitachi Software Engineering Co., Ltd.

Abstract

The authors present an integrated system of multiple Windows environments; one Windows environment is used to process classified information, and the other is used to access Internet and may be infected by computer virus. The authors make use of secure OS and virtual machine, and the two Windows environments are virtually separated at the physical level. As a result, the first Windows environment is not infected by virus, nor classified information will be leaked out to Internet, even if the second Windows environment is infected by unknown virus. The authors describe the system architecture, the separation of the two environments with use of the secure OS, performance and security considerations.

1. はじめに

セキュリティ脅威の中で最も発生件数が高いのはウィルスである．ウィルス対策としては，ワクチンソフトウェアを利用して感染を防ぐのが一般的である．しかし，感染経路がメールの添付ファイルだけではなく，webページに含まれるスクリプトやサービスへの直接攻撃などと多様化したことにより，ウィルスパターンファイルの配布が間に合わず，感染してしまう可能性が大きくなっている．また，メールを使ってトロイの木馬を送りつける場合，ターゲットとなる受信者やその所属組織を特定，受信者の関連業務を件名とするなど，ソーシャルエンジニアリングを利用する手口が現れており，事態が悪化している[1].

ウィルス対策の一つに，セキュアOSがある．セキュアOSは強制アクセス制御や役割ベースのアクセス制御を実現しており，たとえアプリケーションにセキュリティホールがあって攻撃を受けても，被害範囲をそのアプリケーションに閉じ込めることができる．すなわち，バッファオーバーフローなどの方法で攻撃にあっても，アプリケーションに関係のないファイルへのアクセスやシェルを含め関係のないプログラムの起動を防止することができる．しかし，LinuxやSolarisをプラットフォームとする対策が中心[2, 3]であり，Windowsベースのクライアントには適用できないのが現実である．

セキュアOS以外のウィルス対策として，プログラムの振舞をみてウィルスを検知する方法がある[4]．これはウィルススキャンのパターン照合で発見されないように暗号化したコードの復号処理や大量のメール送信処理など，ウィルスが多用する処理パターンを検出してウィルスを検知する方法である．しかし，先に述べた特定の受信者や組織を狙うトロイの木馬は，振舞が固有になる可能性があり，検知できるとは限らない．

一方，最近大きな問題になっているのは，顧客情報他の情報漏洩である．原因としては盗難や紛失が半数以上を占めるが，内部犯罪や不正アクセス，ウィルスなどによる漏洩も発生している．内部犯罪対策については，USBメモリなどの外部媒体を無効化したり，キーワードを用いた電子メールのフィルタリングなどが使用されているが，十分とは言い切れない．

本報告では，未知のウィルス，パターンファイル配布より早く感染が広まるウィルスへの対策

とアクセス権限者の故意の情報持出しを防止する対策とを兼備える二系統 Windows システムの概要や性能, 安全性を示す.

2. 二系統 Windows システム

2.1 全体構成

先の目標を達成するために, 機密情報を扱う機密系 Windows 環境とウィルス感染可能性のある一般系 Windows 環境を分離, 仮想マシンを使って 1 台の PC に統合する. また, 利便性を考慮し, 一部データを一般系 Windows から機密系 Windows にコピーできるようにする. これを実現するため図 1 に示す構成をとる.

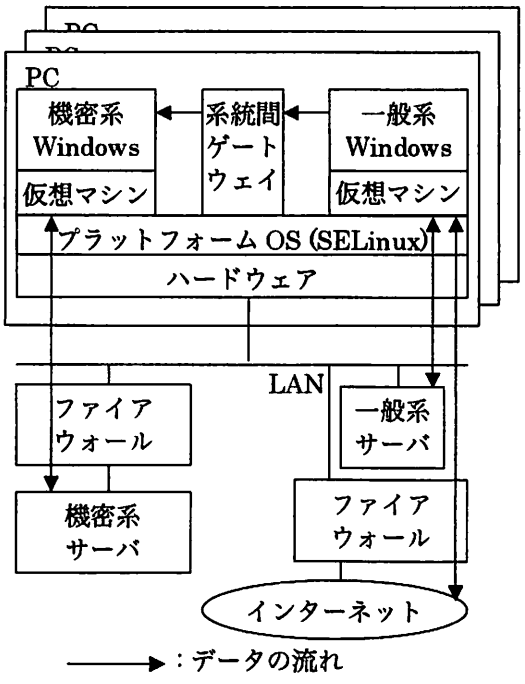

図 1 二系統 Windows システムの構成

プラットフォームとなる OS はシステム全体のベースなので高い安全性が要求される. このため, 原理的に不正なプログラム起動や権限昇格が起きない Security-Enhanced Linux (SELinux) [2]を用いる. SELinux の概要, 本システムへの適用方法については, 第 3 章にて報告する.

プラットフォーム OS 上の仮想マシン上で, 利用者が直接利用する Windows が二つ稼動する. 一つは外部への漏洩が許されない機密情報を扱う機密系 Windows であり, 他はインターネットへのアクセスが可能な一般系 Windows である. 本システムでは仮想マシンとして VMware [5] を利用する.

系統間ゲートウェイは二つの Windows 間の制限されたデータ転送を実現する.

PC を接続する LAN には予め定められた機器だけを接続するようにする. 例えば, ウィルスに感染したり, 利用者が勝手に決めた IP アドレスをもつ PC の接続はないものとする.

2.2 機密系 Windows での漏洩防止

機密系 Windows では, 印刷や外部媒体を用いた漏洩防止策として, プリンタや USB ポート, CD ドライブの使用を禁止する. 具体的には, 既存の漏洩防止ツールを利用する他に, 仮想マシンで USB インタフェースを使えなくする方法がある.

2.3 プラットフォーム OS

利用者の利便性を高めるとともに, 利用者の操作ミスや故意の設定・ファイル変更を防ぐため, プラットフォーム OS や系統間ゲートウェイ, 仮想マシンプログラムへの利用者のアクセスを禁止する. このためには, ハードウェアの電源をオンにすればシステムが起動, 二つの Windows をシャットダウンすればプラットフォーム OS もシャットダウンし, さらにプラットフォーム OS のコンソールへのアクセスを禁止すればよい. 以下のようにプラットフォーム OS を設定して, これを実現する.

(1) デフォルト runlevel を通常未使用の 4 とし, さらに getty の起動を制限する. このために /etc/inittab を変更する.
(2) 以下を起動するスクリプトプログラムをプラットフォーム OS 起動後に一度だけ実行する. これには/etc/inittab に action エントリを once としてスクリプトを登録すればよい.
  (a) X ウィンドウのサーバ
  (b) 系統間ゲートウェイ
  (c) 機密系 Windows と一般系 Windows の仮想マシンプログラム
  (d) X ウィンドウのコンソールへのアクセスを禁止するためのディスプレイサイズの xclock
  (e) 二つの仮想マシンプログラム終了後に(d)を強制終了するプログラム
  (f) (e)の後のプラットフォーム OS のシャットダウンプログラム
(3) PC の管理などに必要なサービスを残し, 不要なネットワークサービスを停止する.

今回利用した仮想マシンではコントロールキーと Alt キーとファンクションキーを組合わせることで, ディスプレイを切替えることできる. 通常は tty0 などの端末切替えに利用するが, 仮想マシンが稼動しているプラットフォーム OS 上の X ウィンドウのコンソールにも切替えられるようになり, 仮想マシンの設定が変更できる. これを防ぐため, フルスクリーンの xclock を起動してキ

ーボードやマウスが使えないようにする．以上により，利用者が直接プラットフォーム OS にアクセスすることができなくなる．

2.4 PC 内のネットワーク構成

一般系 Windows から機密系 Windows へのウィスル侵入防止と逆方向の機密情報漏洩防止のために，二つの Windows 間の通信を原則禁止する必要がある．また，一般系 Windows は従来どおりのインターネットが使える環境とする．さらに，機密系 Windows は機密系ファイルサーバ他の組織内の業務用サーバへのアクセスが必要である．以上の要求を満たすため以下に述べるネットワーク構成をとる．

(1) 仮想マシンの仮想ネットワーク機能を用いて，機密系 Windows と一般系 Windows を別の仮想ネットワークセグメントに接続する．さらに，二つのネットワークセグメントを接続するルータにあたるプラットフォーム OS で二つの Windows 間の直接通信を禁止する．
(2) 機密系 Windows は，プラットフォーム OS の NAT 機能を介してだけ機密系ファイルサーバなどの業務システムにアクセスする．逆にこれらサーバへのアクセスは，機密系 Windows からのアクセスだけを許可する．
(3) 一般系 Windows は，プラットフォーム OS の NAT 機能を介してだけインターネット上の web サーバや一般系メールサーバにアクセスする．また，ウィルスに対しては既存の対策を行い，できる限り感染しないようにする．インターネットからの不正アクセスに対しては，従来通りファイアウォールやアプリケーションプロキシサーバを通じてアクセスする．

2.5 二つの Windows 間のデータ交換

一般系 Windows と機密系 Windows の間の通信を禁止する．しかし，これではインターネット上の web サイトにある情報や電子メールで送られてきたデータを機密文書の一部として利用することが全くできず，不便である．

これを解決，利便性を確保するため，一般系 Windows から機密系 Windows へのクリップボードデータのコピーを許可する．具体的には，一般系 Windows のクリップボードを監視，クリップボードにデータが書き込まれると，データをプラットフォーム OS 上の系統間ゲートウェイを介して機密系 Windows のクリップボードにコピーする．ただし，ファイルコピーは禁止する．

3. セキュア OS の適用

3.1 SELinux の概要

SELinux [2]では，プロセスにドメイン，ファイル他のリソースにタイプというラベル付けを行い，どのドメインのプロセスがどのタイプのリソースにどの種別のアクセスを許可するのかのセキュリティ規則を定める．各ドメインの各タイプへのアクセスを最少限に設定することで，アプリケーションの欠陥を利用して不正コードを SELinux で実行することができても，不正にアクセスできるデータや起動するプログラムをセキュリティ規則で制限した範囲に限定することができる．

先のセキュリティ規則を変更できるのは，sysadm_r という役割を持ち sysadm_t というドメインが使える利用者だけである．デーモンを始め多くのプロセスは sysadm_t タイプを使うことができないので，仮にアプリケーションプログラムにセキュリティホールがあってもセキュリティ規則を変更することはできない．

3.2 セキュリティ規則の設計

本システムに適用した SELinux セキュリティ規則の概要を図 2 に示す．本システムは X サーバと二つの仮想マシンと系統間ゲートウェイの四つの主要なプログラムからなり，それぞれに別のドメインを割当て，さらにアクセスするリソースごとに別のタイプを割当て，各ドメインの各タイプへのアクセス権限を最少限にするようにする．このために，基本的に図 2 に示すように各プログラムと関連するファイルにドメインとタイプを割当てる．以下に概要を示す．

プラットフォーム OS の init プロセスから，X ウィンドウ起動コマンドを用いて X サーバや X クライアントにあたる機密系 Windows が載る仮想マシンと一般系 Windows が載る仮想マシンと系統間ゲートウェイを起動する．X ウィンドウ起動コマンド自体，init プロセスとは別ドメイン sw_t とし，さらにそれぞれの X クライアントを別ドメインとする．

仮想マシンがアクセスする主なリソースには，ログファイル，設定ファイル，仮想ディスクファイルの 3 種類があり，それぞれのアクセス種別は，追記，読込み，読み書きとする．機密系と一般系，さらにアクセス種別ごとに個別のタイプを割当て，必要最少の権限を与えるようにする．

4. 性能

上記設計に従った二系統 Windows システムを実現，表 1 に示す環境で起動時間を測定したところ，SELinux と X サーバの起動までに約 75 秒，二つの Windows のログイン画面表示までに約 185 秒かかる．速いとはいえないが，実用になる時間といえる．

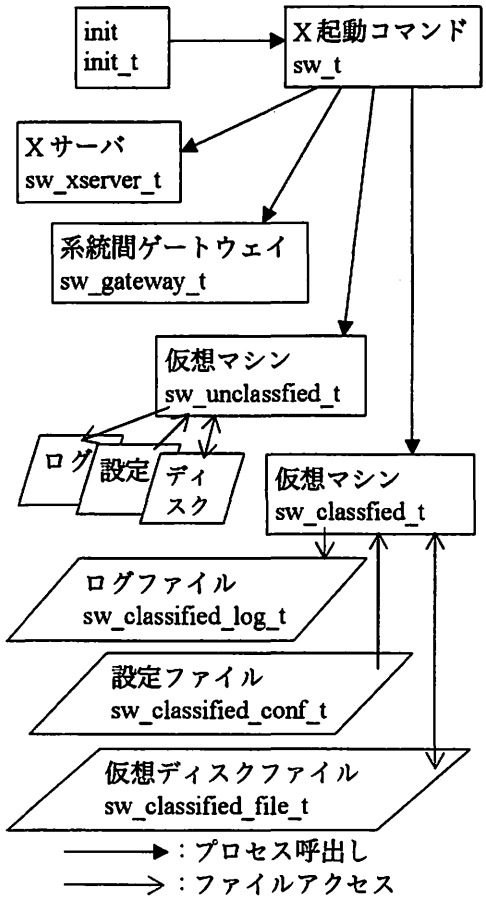

図2 SELinuxセキュリティ規則

表1 性能測定環境

#	項 目	内 容
1	SELinux	Fedora Core 2
2	仮想マシン	VMware Workstation 4.5
3	Windows	Windows 2000 Pro. + SP4
4	CPU	Pentium 4 (3GHz)
5	メモリ	2GB

また CrystalMark 0.9.114 [6]を用いてベンチマーク評価を行った結果を表2に示す.

表2 通常 Windows との性能比較

#	比較項目	同時	単独	Win
1	整数演算	6,213	6,040	6,432
2	浮動小数点演算	7,608	7,342	4,804
3	メモリアクセス	5,559	5,250	7,112
4	HD アクセス	17,338	34,768	5,521
5	2D 描画	2,951	2,231	2,545

同時というのは一般系 Windows と機密系 Windows 同時に計測した時の平均値. 単独は片方の Windows での計測値, Win は CPU が Pentium 4 (2.26GH), メモリが 1GB の PC 上の仮想マシンを用いない通常の Windows 2000 Pro. + SP4 での計測値である. 二系統 Windows と通常の Windows を比較すると, ハードディスクアクセス(HD アクセス)を除いて大きくは異ならない数値が出ている. 二系統 Windows の方が HD アクセスの数値が良いのは, ファイル I/O をプラットフォーム OS か仮想マシンがキャッシュしているためと考えられる. また別の測定では, 通常の Windows と比較すると VMware 上の Windows の 2D 描画は 4 割程度低下するが, 整数演算やメモリアクセスの低下は 1 割程度である.

5. 安全性の検討

5.1 インターネットからの攻撃

ワームやトロイの木馬を含めたウィルスの侵入経路として, 第一にインターネットが考えられる. インターネットにアクセスする一般系 Windows が未知のウィルスに感染したとしても, 機密系 Windows までには拡がらない. これは, 一般系 Windows がアクセスできる範囲が一般系サーバまでであり, 機密系 Windows や機密系サーバへのアクセス経路がないためである.

系統間ゲートウェイを介したデータ交換では, 一般系 Windows で利用者が目視して選択したデータをクリップボードにコピー, 本データが自動的に系統間ゲートウェイを介して機密系 Windows のクリップボードにコピーされ, 機密系 Windows で利用者がアプリケーションに貼り付ける. 利用者が目視できる文書中のテキストや図表が対象なので, ウィルスのコードが実行可能な形で機密系 Windows に持ち込まれる可能性は非常に低いと考えられる. しかし, ウィルス自身が長大データ, 異常値を含んだデータをクリップボードにコピーし, 貼り付けた際にバッファオーバーフロー他の攻撃が起こる可能性が残る. 対策として以下がある.

(1) データ形式ごとのウィルスチェック
(2) 一般系 Windows でクリップボードデータをイメージデータに変換, プラットフォーム OS ないしは機密系 Windows で元の形式に変換して, 上記攻撃が起きないようにする.

5.2 リソース消費型ウィルス

一般系 Windows に対して, CPU やネットワーク, ディスクリソースを消費するウィルスの攻撃があり得る. 対策として以下がある.

(1) プラットフォーム OS で個別の仮想マシンが利用するリソースを監視, 上限を設ける.
(2) 一般系 Windows でリソースを監視する. しかし, ウィルスに監視プログラムが攻撃される可能性が残る.

(3) ネットワークリソース保護のため，機密系と一般系とネットワーク回線レベルから完全に分離する．PC のネットワークインタフェースカード(NIC)も二枚挿し，それぞれの仮想マシンがアクセスする NIC もプラットフォーム OS で制限する．

5.3 通信データの盗聴他

機密系 Windows と機密系サーバとの通信での詐称，盗聴，改竄が考えられる．対策として IPsec や TLS を使った暗号認証通信がある．特に前提にある「許可機器のみが LAN に接続」が達成できない場合には，通信相手の認証は必須となる．

5.4 仮想マシンの欠陥

仮想マシンに欠陥があり，特殊なコードを実行すると，プラットフォーム OS 上のファイルを破壊したり勝手にプロセスを起動するかもしれない．しかし，プラットフォーム OS の強制アクセス制御により，仮想マシンのプロセスがアクセスできるファイルや起動できるプログラムは制限されており，プラットフォーム OS の脆弱性やセキュリティ規則の間違いを利用できない限り，攻撃は失敗する．

5.5 ウィルスの自作

機密系 Windows で利用者がウィルスを自作すれば，他の PC 上の機密系 Windows に感染したり，機密系サーバに感染したりする．

攻撃対象となるセキュリティホールにパッチを当てるのは有効な対策となるが，自作のオリジナルなウィルスなら既存のウィルス対策の効果は薄い可能性が高く，万全な対策はない．

5.6 物理的系統分離との比較

セキュリティに厳格な組織では，従来からネットワーク回線，ネットワーク機器，PC まで複数系統に分離する構成をとって，情報の漏洩や組織外部からの不正侵入を防いできた．このような構成と比較すると本システムでは，以下の弱点がある．

(1) 5.1 に示したクリップボード経由のウィルス侵入の可能性が残る．
(2) 5.2 に示したリソース消費型ウィルスに弱い．

逆に利点としては以下がある．

(1) オフィスのスペース効率向上
(2) クリップボードデータコピーによる利便性向上
(3) ハードウェア共有による導入コストの削減

(1)に関しては，組織によっては一人で 3 台，4 台の PC を利用している利用者も存在しており効果が大きいと言える．

6. 類似研究

セキュリティ向上のために一台の PC に複数 OS が稼動するシステムとしてナノカーネルを用いたヒステリシス署名システムがある[7]．ナノカーネル上に利用者 OS とセキュリティ OS が稼動，利用者 OS 上の署名要求プログラムがセキュリティ OS 上の署名プログラムを呼出す．署名鍵や署名履歴はセキュリティ OS だけがアクセスでき，利用者 OS からはアクセス不能である．セキュリティ上重要なデータを，そのアクセス手段を含めて利用者が利用している OS とは別の安全な OS 上に移して安全性を向上している．

一方，本研究では Windows やインターネットなど既存の利用環境を維持しながら，未知のウィルスを含めた攻撃から業務上重要で機密性の高い情報を，従来の使い勝手を維持しつつ保護している．

7. まとめ

機密情報を扱う Windows 環境とインターネットアクセス可能でウィルス感染の可能性がある Windows 環境を，セキュア OS と仮想マシンを使い一台の PC に統合した．二つの Windows 環境はセキュア OS を使って分離した仮想マシン上で稼動し，原理的に一般系 Windows から機密系 Windows にウィルスが侵入したり，逆方向に機密情報が漏洩することはなく，機密系にて安全な Windows 環境を保障することができる．さらに，物理的に PC やネットワークの系統を分けた場合に比べ，スペース効率や利便性が向上した．

謝辞

本システムの安全性検討にあたり横浜国立大学大学院環境情報学院松本勉教授にご協力頂きました．ここに謝意を表します．

参考文献

[1] http://jvn.jp/tr/TRTA05-189A/
[2] http://www.nsa.gov/selinux/
[3] http://www.argus-systems.com/public/docs/pitbull.whitepaper.oss.pdf
[4] Mihai Christodorescu, Somesh Jha, Sanjit Seshia, Dawn Song, and Randal E. Bryant: Semantics-Aware Malware Detection, 2005 IEEE Symposium on Security and Privacy (May 2005)
[5] http://www.vmware.com/
[6] http://www.CrystalMark.info/
[7] 伊藤 信治, 宮崎 邦彦, 吉浦 裕, 谷本 幸一: 複数 OS 環境を利用したヒステリシス署名システムの実装, 情報処理学会 コンピュータセキュリティシンポジウム 2002 (Oct. 2002)